UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/063,996	06/03/2002	David Carroll Challener	RPS920020055	7193

25299 7590 02/13/2006

IBM CORPORATION
PO BOX 12195
DEPT YXSA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER
DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/063,996	**Applicant(s)** CHALLENER ET AL.	
	Examiner Zachary A. Davis	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 03 June 2002.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-12 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-12 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 03 June 2002 is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 20020603.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: diskette 10 (see page 8, paragraph 0027 of the present specification).

2. The drawings are objected to because the drawings, specifically Figure 3, include grayscale shading that makes labels difficult to read and at least partially illegible.

3. Figure 4 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

4. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New

Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

5. The Examiner further recommends that reference numerals be added, especially to the flowcharts of Figures 1 and 2, and to the corresponding portions of the description, in order to increase the clarity of the disclosure.

Specification

6. The disclosure is objected to because of the following informalities:

The specification makes reference to the Trusted Computing Platform Alliance (TCPA) glossary of terminology (see page 2, paragraph 0003 of the present specification); however, Applicant has not provided a copy of the TCPA glossary, nor indicated which version of the specification and glossary is to be considered. Therefore, it is not clear exactly which version of the glossary definitions are intended in the present specification.

The specification refers to a prior application that is only identified by filing date and title (see page 3, paragraph 0008 of the present specification). It is not clear to which application this refers, although it appears that it may refer to Application No. 10/144,200. Applicant is required to definitively identify the application by serial number (or patent number, if issued).

The specification appears to contain minor typographical and other errors. For example, on page 7, at line 4 of paragraph 0024, it appears that "the one to which is it specifically bound" is intended to read "the one to which it is specifically bound", and on page 7, at line 3 of paragraph 0025, it appears that "a keys" is intended to read simply "keys".

Appropriate correction is required. The above is not to be considered an exhaustive list of errors. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

Claim Objections

7. Claims 1-12 are objected to because of the following informalities: The claims are not properly numbered. The format of "[c1]" for Claim 1, for example, is not acceptable. Claims should be numbered with the numeral followed by a period, e.g. "1." Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 3-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 3 recites the limitation "the trusted platform module endorsement key" in lines 19-20 of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the TPM endorsement public key" in lines 7-8 of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claims 5 and 7 recite the abbreviation "TPM". While it appears that this is intended to represent "trusted platform module", the abbreviation is not defined in these claims, rendering them potentially indefinite.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1 and 2 are rejected under 35 U.S.C. 102(b) as being anticipated by Olarig et al, US Patent 6032257, and Parzych et al, US Patent 5375243 (Olarig, column 1, lines 47-49, where Parzych is incorporated by reference).

In reference to Claims 1 and 2, Olarig and Parzych disclose a method including executing program instructions to initiate system operation (see Olarig, column 7, line 60-column 8, line 10), identifying the presence of a hard disk drive (HDD) (Olarig, column 6, lines 51-53), reading a public key and storing the public key in a read only area of the HDD (Olarig, column 5, lines 64-67; and column 9, lines 29-31), prompting a user to enter a password for controlling access to the HDD (see Parzych, column 7, lines 36-37 and column 7, line 66-column 8, line 14), and generating a hash value from the password and storing the hash value in a protected area of the HDD to control access to the HDD (Parzych, column 8, lines 27-41, where the password is encrypted; see also Olarig, column 9, lines 27-29, where a digital signature is used, noting, see Olarig, column 2, lines 58-65, that a signature include a message digest or hash).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 3-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olarig et al and Parzych et al (Olarig incorporates Parzych by reference, see Olarig, column 1, lines 47-49) in view of Menezes et al, *Handbook of Applied Cryptography*.

In reference to Claims 3 and 4, Olarig and Parzych disclose a method including executing program instructions to initiate system operation (see Olarig, column 7, line 60-column 8, line 10), distinguishing between a requirement for entry of at least one password for access to a hard disk drive (HDD) and no requirement for entry of a password (see Parzych, column 4, lines 5-29), prompting an operator to enter a password if it is required (Parzych, column 9, lines 5-6), extending the password to a register (Parzych, column 9, lines 7-10), quoting the register contents to the HDD (Parzych, column 9, lines 11-23), verifying that the quoted contents are derived from the password and a public key (Olarig, column 8, lines 22-27; see also column 9, lines 27-29 where a digital signature is verified), and granting access on verification (Parzych, column 9, lines 23-25). However, Olarig and Parzych do not explicitly disclose the use of a nonce string with the password.

Menezes discloses that a nonce is used in an authentication or identification protocol in order to prevent replay attacks (pages 397-398, Section 10.3.1, noting especially Definition 10.9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Olarig and Parzych to include the use of a nonce in order to prevent replay attacks (see Menezes, page 397).

In reference to Claims 5 and 6, Olarig and Parzych disclose a method including, on installation of a hard disk drive (HDD), executing program instructions to initiate system operation (see Olarig, column 7, line 60-column 8, line 10), identifying the presence of an HDD (Olarig, column 6, lines 51-53), storing a public key in a read only area of the HDD (Olarig, column 5, lines 64-67, and column 9, lines 29-31), prompting a user to enter a password for controlling access to the HDD (see Parzych, column 7, lines 36-37 and column 7, line 66-column 8, line 14), and generating a hash value from the password and storing the hash value in a protected area of the HDD to control access to the HDD (Parzych, column 8, lines 27-41, where the password is encrypted; see also Olarig, column 9, lines 27-29, where a digital signature is used, noting, see Olarig, column 2, lines 58-65, that a signature include a message digest or hash). Olarig and Parzych further disclose, on subsequent powering on of the system, executing program instructions to initiate system operation (see Olarig, column 7, line 60-column 8, line 10), prompting an operator to enter a password (Parzych, column 9, lines 5-6), extending the password to a register (Parzych, column 9, lines 7-10), quoting the register contents to the HDD (Parzych, column 9, lines 11-23), verifying that the quoted contents are derived from the password and a public key (Olarig, column 8, lines 22-27; see also column 9, lines 27-29 where a digital signature is verified), and granting access on verification (Parzych, column 9, lines 23-25). However, Olarig and Parzych do not explicitly disclose the use of a nonce string with the password.

Menezes discloses that a nonce is used in an authentication or identification protocol in order to prevent replay attacks (pages 397-398, Section 10.3.1, noting especially Definition 10.9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Olarig and Parzych to include the use of a nonce in order to prevent replay attacks (see Menezes, page 397).

In reference to Claims 7 and 8, Olarig and Parzych disclose an apparatus including a computer system and hard disk drive (HDD) where a public key is stored in the HDD (Olarig, column 5, lines 64-67, and column 9, lines 29-31) and which identifies the system and HDD as being specifically linked (Olarig, column 5, line 64-column 6, line 4). Olarig and Parzych further disclose the system performing operations including prompting an operator to enter a password (Parzych, column 9, lines 5-6), generating a value from the password and the key (Parzych, column 8, lines 27-41, where the password is encrypted; see also Olarig, column 9, lines 27-29, where a digital signature is used, noting, see Olarig, column 2, lines 58-65, that a signature include a message digest or hash), supplying the value to the HDD (Parzych, column 9, lines 11-23), verifying that the value is derived from the password and key (Olarig, column 8, lines 22-27; see also column 9, lines 27-29 where a digital signature is verified), and granting access to the device on verification (Parzych, column 9, lines 23-25). However, Olarig and Parzych do not explicitly disclose the use of a nonce string with the password.

Menezes discloses that a nonce is used in an authentication or identification protocol in order to prevent replay attacks (pages 397-398, Section 10.3.1, noting especially Definition 10.9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Olarig and Parzych to include the use of a nonce in order to prevent replay attacks (see Menezes, page 397).

In reference to Claims 9 and 10, Olarig, Parzych, and Menezes disclose that the device can be internal or external (see Olarig, column 6, line 51-column 7, line 19).

Claims 11 and 12 are directed to software implementations of methods corresponding substantially to the methods of Claims 3 and 5, and are rejected by a similar rationale.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Angelo, US Patent 5887131, discloses a method for controlling access to, for example, a hard drive, including comparing hashes of passwords.

b. Liebenow, European Patent Application Publication EP 0770997, discloses a system for password protection of a removable hard drive.

c. Menezes, *Handbook of Applied Cryptography*, also discloses storing “encrypted” hashes of passwords (see page 389).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER